

In re Patent Application of:

DELOW ET AL.

Serial No. 10/817,148

Filed: **APRIL 2, 2004**

REMARKS

Applicants thank the Examiner for the careful and thorough examination of the present application, and for correctly withdrawing the previous rejections of the claims. Applicants submit that all claims are patentable and present arguments herein supporting such patentability.

I. The Claimed Invention

Independent Claim 1 is directed to a semiconductor integrated circuit to execute application code to be received from a memory via external connections. The integrated circuit comprises a processor to execute the application code from the memory, an internal bus to provide the application code to the processor from the memory, and a verifier processor. The verifier processor is to receive the application code via the internal bus and continually processes the application code using a verification function while the processor executes the application code from the memory independently of the verifier processor. The verifier processor is also for impairing the function of the integrated circuit in an event that the application code does not satisfy the verification function. The integrated circuit further comprises an instruction monitor to monitor code requests issued by the processor and to impair the function of the integrated circuit unless addresses of the code requests fall within a given range.

Independent Claim 19 is similar to Claim 1, but recites the verifier processor processes the application code, and the

In re Patent Application of:

DELOW ET AL.

Serial No. **10/817,148**

Filed: **APRIL 2, 2004**

instruction monitor is connected to the internal bus.

Independent Claim 25 is directed to a system combination of the semiconductor integrated circuit of Claim 19, and a non-volatile memory that stores application code. Independent Claim 31 is a method counterpart to Claim 1.

II. The Claims Are Patentable

The Examiner rejected independent Claims 1, 19, 25, and 31 over Warren in view of Goffin et al. Warren discloses an integrated circuit comprising a CPU, a bus coupled to the CPU, a memory coupled to the bus, a breakpoint range unit storing first and second breakpoint addresses, and a logic controller coupled to the breakpoint range unit. The breakpoint range unit compares the instruction address currently being processed by the CPU. If the current instruction address falls within the first and second breakpoint addresses, the breakpoint range unit generates a breakpoint signal, which is received by the logic controller. Upon receipt of the breakpoint signal, the logic controller interrupts the CPU, thereby enabling diagnostic tests on the CPU. (Col. 2, lines 25-47).

The Examiner correctly notes that Warren fails to disclose the verifier processor continually processing the application code using a verification function while the processor executes the application code from the memory independently of the verifier processor, as recited, for example, in independent Claim 1. The Examiner looks to Goffin et al. to supply this deficiency of Warren.

In re Patent Application of:

DELOW ET AL.

Serial No. **10/817,148**

Filed: **APRIL 2, 2004**

Goffin et al. discloses a computing device that includes a master processor, a master memory unit coupled to the master processor via a memory bus, and a secure processor also coupled to the memory via the memory bus. (Figure 1). The code is first downloaded by the master processor and stored in the master memory unit for subsequent authentication by the secure processor. (Page 10, line 32 through Page 12, line 12). The secure processor receives the code via the memory bus. (Page 12, lines 1-3). If the code is not authentic, the secure processor can erase or disable the adulterated memory blocks or disable the entire computing device. (Page 13, lines 12-18). The secure processor may periodically sweep code stored in the master memory unit for re-authentication. (Page 14, lines 5-16).

In an alternative embodiment, the code is initially received by the secure processor rather than the master processor. In this embodiment, the secure processor receives the code and stores it in an interim memory before long-term storage of authenticated code in the master memory unit. (Page 12, lines 13-23). Goffin et al. does not disclose how the secure processor receives the code directly.

Applicants submit that Goffin et al. fails to disclose the verifier processor receiving the application code via the internal bus, and the processor executing the application code from the memory independently of the verifier processor, as recited in independent Claim 1. In the first embodiment, i.e. where the master processor first receives code and stores it for subsequent authentication, the verification routine is not

In re Patent Application of:

DELOW ET AL.

Serial No. **10/817,148**

Filed: **APRIL 2, 2004**

independent from the master processor since it first receives the code for storage. In the second embodiment, i.e. where the secure processor receives the code first, the code is not received via the memory bus, as in the first embodiment. In other words, Goffin et al. fails to disclose both the verifier processor receiving the application code via the internal bus, and the processor executing the application code from the memory independently of the verifier processor, as recited in independent Claim 1. For this reason alone, independent Claim 1 is patentable over the prior art.

Applicants also note that Goffin et al. fails to disclose the verifier processor continually processing the application code using a verification function while the processor executes the application code from the memory independently of the verifier processor. Differently, in Goffin et al., the authentication of the code by the secure processor is sequentially performed before any execution by the master processor. Moreover, even during re-authentication, the secure processor gives way to the master processor's use of the memory bus, for example, when the master processor is accessing code for execution. (Page 14, line 17 through Page 15, line 8). Therefore, for this additional reason, independent Claim 1 is patentable over the prior art.

The Examiner's stated motivation to combine Warren with Goffin et al. was that the person of ordinary skill in the art would modify Warren as suggested to increase security of the system. Applicants submit that the Examiner's combination is

In re Patent Application of:

DELOW ET AL.

Serial No. **10/817,148**

Filed: **APRIL 2, 2004**

improper because the prior art references teach away from such a selective combination. More particularly, Warren discloses an integrated circuit for diagnostic procedures, i.e. interrupting normal operation of the CPU to allow diagnostic procedures to be implemented. (Col. 1, lines 5-8). Differently, Goffin et al. discloses a computing device that provides for secure downloading of software. (Page 1, lines 8-25). Given that Warren deals with diagnostics and not security, Applicants submit that the person of ordinary skill in the art would be taught away from the Examiner's proposed selective combination.

Accordingly, because of the above noted critical deficiencies of the prior art, independent Claim 1 is patentable over the prior art. Independent Claims 19, 25, and 31 are similar to Claim 1 and are patentable for similar reasoning. Their respective dependent claims, which recite yet further distinguishing features, are also patentable over the prior art and require no further discussion herein.

In re Patent Application of:

DELOW ET AL.

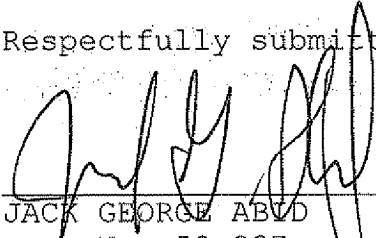
Serial No. **10/817,148**

Filed: **APRIL 2, 2004**

CONCLUSION

In view of the arguments provided herein, it is submitted that all the claims are patentable. Accordingly, a Notice of Allowance is requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,



JACK GEORGE ABUD
Reg. No. 58,237
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330
407-841-2343 fax
Attorney for Applicants